SAP Dispute Management 6.0

Copyright

Icons in Body Text

Icon	Meaning
	Caution
	Example
	Note
	Recommendation
	Syntax

Additional icons are used in SAP Library documentation to help you identify different types of information at a glance. For more information, see *Help on Help → General Information Classes and Information Classes for Business Information Warehouse* on the first page of any version of *SAP Library*.

Typographic Conventions

Type Style	Description
Example text	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation.
Example text	Emphasized words or phrases in body text, graphic titles, and table titles.
EXAMPLE TEXT	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
`Example text`	Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
Example text	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
<Example text>	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
EXAMPLE TEXT	Keys on the keyboard, for example, F2 or ENTER.

SAP Dispute Management 6.0

Introduction

This guide does **not** replace the daily operations handbook that we recommend customers to create for their specific productive operations.

Target Group

- Technology consultants
- System administrators

This document is **not** included as part of the Installation Guides, Configuration Guides, Technical Operation Manuals, or Upgrade Guides. Such guides are only relevant for a certain phase of the software life cycle, whereby the Security Guides provide information that is relevant for all life cycle phases.

The Need for Security

With the increasing use of distributed systems and the Internet for managing business data, the demands on security are also on the rise. When using distributed systems, you need to be sure that your data and processes support your business needs without allowing unauthorized access to critical information. User errors, negligence, or attempted manipulation of your system must **not** result in loss of information or processing time. These security requirements also apply to *SAP Dispute Management*. To assist you in securing *SAP Dispute Management*, we provide this Security Guide.

About this Document

The Security Guide provides an overview of the security-relevant information that applies to *SAP Dispute Management*.

Overview of the Main Sections

The Security Guide comprises the following main sections:

- **Before You Start**

  This section contains information about why security is necessary, how to use this document, and references to other Security Guides that build the foundation for this Security Guide.

- **Technical System Landscape**

  This section provides an overview of the technical components and communication paths that are used by the *SAP Dispute Management*.

- **User Management and Authentication**

  This section provides an overview of the following user management and authentication aspects:

  - Recommended tools for user management.
  - User types required for *SAP Dispute Management*
  - Standard users delivered with *SAP Dispute Management*
  - Overview of integration options in Single Sign-On environments

- **Authorizations**

  This section provides an overview of the authorization concept that applies to *SAP Dispute Management*.

- **Network and Communication Security**

  This section provides an overview of the communication paths used by *SAP Dispute Management* and the security mechanisms that apply. It also includes our recommendations for the network topology to restrict access at the network level.

- **Data Storage Security**

  This section provides an overview of any critical data that is used by *SAP Dispute Management* and the security mechanisms that apply.

Before You Start

Fundamental Security Guides

SAP Dispute Management is based on *SAP NetWeaver* and *mySAP ERP*. Therefore, the corresponding Security Guides also apply to *SAP Dispute Management*. Pay particular attention to the most relevant sections or specific restrictions as indicated in the table below.

Fundamental Security Guides

Scenario, Application or Component Security Guide	Most-Relevant Sections or Specific Restrictions
SAP NetWeaver Security Guide	Security Aspects for Connectivity and Interoperability
SAP ERP Central Component Security Guide	
Financial Basis Security Guide	

For a complete list of all of the Security Guides published by SAP, see SAP Service Marketplace at **`service.sap.com/securityguide`**.

Additional Information

For more information about special topics, see the sources listed in the table below.

Further Information

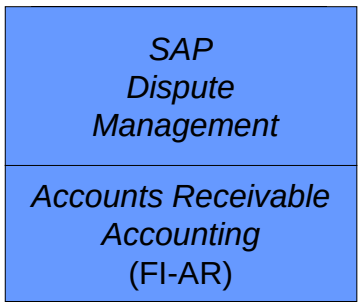
Content	SAP Service Marketplace
Security	service.sap.com/security
Security Guides	service.sap.com/securityguide
Related SAP Notes	service.sap.com/notes
Platforms permitted	service.sap.com/platforms
Network security	service.sap.com/network service.sap.com/securityguide
Technical infrastructure	service.sap.com/ti
SAP Solution Manager	service.sap.com/solutionmanager

Technical System Landscape

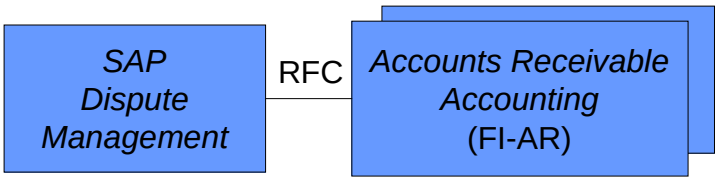
Use

You can use *SAP Dispute Management* as a **one-system** or as a **multiple-system scenario**. If you use *SAP Dispute Management* in a one-system scenario, this means that you use *SAP Dispute Management* in the same system as Accounts Receivable. In a multiple-system scenario, you run *SAP Dispute Management* in a separate system. This communicates with the Accounts Receivable system connected by means of synchronous and asynchronous BAPI calls and dialog calls.

The following figure shows an overview of the technical system landscape of *SAP Dispute Management* in a one-system scenario.



The following figure shows an overview of the technical system landscape of *SAP Dispute Management* in a multiple-system scenario.



For more information about the technical system landscape, see the sources listed in the table below.

More Information About the Technical System Landscape

Subject	Guide/Tool	SAP Service Marketplace
Technical configuration High Availability	*Technical Infrastructure Guide*	service.sap.com/ti
Security		service.sap.com/security

User Management and Authentication

SAP Dispute Management uses the mechanisms for user management and authentication provided by the platform *SAP NetWeaver*. Therefore, the corresponding security recommendations and guidelines of the user management and authentication for *SAP NetWeaver* also appy to *SAP Dispute Management*.

In addition to these guidelines, we include information about user management and authentication that specifically applies to *SAP Dispute Management* in the following topics:

- User Management [Seite 8]

  This topic lists the tools to use for user management, the types of users required, and the standard users that are delivered with *SAP Dispute Management.*

- Integration with Single-Sign-On Environments [Seite 10]

  This topic describes how *SAP Dispute Management* supports Single Sign-On mechanisms.

User Management

Use

The user managment of *SAP Dispute Management* uses the mechanisms provided by *SAP NetWeaver*, for example, tools, user types, and password concept. The following sections provide you with an overview of how these mechanisms affect *SAP Dispute Management*. Furthermore, the system outputs a list of standard users that are required for operating *SAP Dispute Management*.

User Administration Tools

The following table shows the user management tools for *SAP Dispute Management*.

User Management Tools

Tool	Detailed Description	Prerequisites
User and role maintenance of *SAP NetWeaver* (transactions `SU01` and `PFCG`)	For more information, see Users and Roles (BC-SEC-USR) [Extern].	

User Types

It is often necessary to create different security policies for different types of users. For example, your policy may specify that users who perform their tasks interactively have to change their passwords on a regular basis, but not those users who perform their tasks using background processing.

Examples of user types required for *SAP Dispute Management*:

- Individual users:
  - For each individual user in your system, you need dialog users for the following purposes:
    - To use the system via *SAP GUI for Windows*
    - If you use *SAP Dispute Management* in a multiple system scenario and the RFC destinations used use a trusted-trusting system relationship, calls to the other system are performed using the current user from the calling system. Therefore, for each user a valid user must also exist in the target system.
- Technical users:
  - Background users can be used for processing in the background.
  - If you use *SAP Dispute Management* in a multiple system scenario and the RFC destinations concerned are configured such that they do **not** use a trusted-trusting system relationship, you need the following technical users for the RFC destinations:
    - Communication users are used for synchronous and asynchronous BAPI calls (IDocs).
    - Dialog users are used for dialog calls that take place remotely in the other system.

For more information about these user types, see the Security Guide for *SAP NetWeaver* under User Types.

Standard Users

If you use *SAP Dispute Management* in a multiple system scenario and there is **no** trusted-trusting system relationship between the systems involved, you have to configure corresponding users for the RFC communication between the systems involved.

Note that in *SAP Dispute Management*, asynchronous BAPI calls, synchronous BAPI calls, and dialog calls take place between the systems involved. There are calls from the Dispute Case Processing system to the system for Accounts Receivable Accounting and vice versa.

The following table shows the users required if you use *SAP Dispute Management* in a multiple system scenario and there is **no** trusted-trusting system relationship between the systems involved.

Standard Users

System	User ID	Type	Password	Description
System for Dispute Case Processing	Example: ALEREMOTE1_COM	Communi-cation users	The user ID and password are stored in the RFC destination for the connection.	These users are used when synchronous or asynchronous BAPI methods are called from the Accounts Receivable system in the Dispute Case Processing system.

System for Dispute Case Processing	Example: ALEREMOTE1_DIA	Dialog users	The user ID and password are stored in the RFC destination for the connection.	This user is used for dialog calls from the Accounts Receivable Accounting system in the Dispute Case Processing system.
Accounts Receivable Accountiing system	Example: ALEREMOTE2_COM	Communi-cation users	The user ID and password are stored in the RFC destination for the connection.	These users are used when synchronous or asynchronous BAPI methods are called from the Dispute Case Processing system in the Accounts Receivable system.
Accounts Receivable Accountiing system	Example: ALEREMOTE2_DIA	Dialog users	The user ID and password are stored in the RFC destination for the connection.	This user is used for dialog calls from the Dispute Case Processing system in the Accounts Receivable Accounting system.

Create the users and enter them in the corresponding RFC destinations. You can assign user IDs as required. The user IDs above are merely examples.

Integration with Single Sign-On Environments

Use

SAP Dispute Management uses the Single Sign-On (SSO) mechanisms provided by *SAP NetWeaver*. Therefore, the security recommendations and guidelines for user management and authentication described in the *SAP NetWeaver Security Guide* also apply to *SAP Dispute Management*.

The *Secure Network Communications* (SNC) mechanism is supported. SNC is available for user authentication and provides an SSO environment when the *SAP GUI for Windows* or *Remote Function Calls* (RFC) are used.

For more information, see *Secure Network Communications* (SNC) in the *SAP NetWeaver* Security Guide.

Authorizations

Use

SAP Dispute Management uses the authorization concept provided by *SAP NetWeaver*. Therefore, the corresponding security recommendations and guidelines for authorizations also appy to *SAP Dispute Management*.

The *SAP NetWeaver* authorization concept is based on assigning authorizations to users based on roles. For role maintenance in *SAP NetWeaver* use the profile generator (transaction PFCG).

Standard Roles

The following table shows the standard roles used by *SAP Dispute Management*.

Role	Description
SAP_FIN_FSCM_DM_USER • One-system and multiple-system scenario	*FSCM Dispute Management - Processor* Contains the authorizations that an end user requires in Dispute Case Processing.
SAP_FIN_FSCM_DM_RFC_COMM • Multiple-system scenario	*RFC user (communication) in Dispute Case Processing* Contains the authorizations required by a user to call synchronous and asynchronous BAPI methods from the Accounts Receivable system in the Dispute Case Processing system. Examples of such methods are creating dispute cases from Accounts Receivable and automatically changing dispute cases using clearing transactions in Accounts Receivable.
SAP_FIN_FSCM_DM_RFC_DIALOG • Multiple-system scenario	*RFC user (dialog) in Dispute Case Processing* Contains the authorizations for a user with which the DISPLAY method is called in the Dispute Case Processing system from the Accounts Receivable system by RFC. The role contains the authorizations necessary for displaying the dispute case.
SAP_FIN_FSCM_DM_AR_DIALOG • One-system scenario	*Role for functions of Accounts Receivable* Contains authorizations required by end users in Dispute Case Processing so that they can call Accounts Receivable functions in Dispute Case Processing. Examples of such functions are including open items in a dispute case and navigating from a dispute case to a linked line item.

SAP_FIN_FSCM_DM_AR_RFC_DIALOG • Multiple-system scenario	*RFC user (dialog) in Accounts Receivable* Contains the authorizations required by a user to call *SAP Dispute Management* dialog methods using RFC from the Dispute Case Processing system in the Accounts Receivable system. Examples of such methods are including open items in a dispute case and navigating from a dispute case to a linked line item.
SAP_FIN_FSCM_DM_AR_RFC_COMM • Multiple-system scenario	*RFC user (communication) in Accounts Receivable* Contains the authorizations required by a user to call *SAP Dispute Management* synchronous and asynchronous BAPI methods from the Dispute Case Processing system in the Accounts Receivable system. Examples of such methods are the automatic write off of dispute cases and automatic notification of Accounts Receivable when confirming and voiding cases.
SAP_FIN_FSCM_DM_DIALOG • One-system scenario	*Role for functions of Dispute Case Processing* Contains authorizations required by end users in Accounts Receivable so that they can call Dispute Case Processing functions in Accounts Receivable. Examples of such functions are creating/displaying dispute cases from transactions in Accounts Receivable and automatically changing dispute cases using clearing transactions in Accounts Receivable.
SAP_BC_CM_ADMINISTRATOR • One-system and multiple-system scenario	*Administrator in Case Management* Since the component *Case Management* represents the base of *SAP Dispute Management*, you also require special *Case Management* authorizations when setting up *SAP Dispute Management*. These are included in this role.

Network and Communication Security

Your network infrastructure is extremely important in protecting your system. Your network needs to support the communication necessary for your business and your needs without allowing unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (at both the operating system and application level) or network attacks such as eavesdropping. If users cannot log on to your application or database servers at the operating system or database layer, then there is no way for intruders to compromise the machines and gain access to the backend system's database or files. Additionally, if users are not able to connect to the server LAN (*local area network*), they cannot exploit well-known bugs and security holes in network services on the server machines.

The network topology for *SAP Dispute Management* is based on the topology used by the *SAP NetWeaver* platform. Therefore, the security guidelines and recommendations described in the *SAP NetWeaver Security Guide* also apply to *SAP Dispute Management*. Details that specifically apply to *SAP Dispute Management* are described in the following topics:

- Security of Communication Channels [Seite 13]

  This section describes the communication paths and logs used by *SAP Dispute Management*.

- Network Security [Seite 14]

  This section describes the network topology recommended for *SAP Dispute Management*. It shows the appropriate network segments for the various client and server components and where to use firewalls for access protection. It also includes a list of the ports needed to operate *SAP Dispute Management*.

- Communication Destinations [Seite 14]

  This topic describes the information needed for the various communication paths, for example, which users are used for which communications.

For more information, see the following sections in the *SAP NetWeaver* Security Guide:

- *Network and Communication Security*
- *Security Aspects for Connectivity and Interoperability*

Communication Channel Security

The following table contains the communication paths used by *SAP Dispute Management,* the protocol used for the connection, and the type of data transferred.

Communication Paths	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front end client using *SAP GUI for Windows* to application server	DIAG	All application data	Passwords
Application server to application server	RFC	Application data	

DIAG and RFC connections can be protected using Secure Network Communications (SNC). HTTP connections are protected using the Secure Sockets Layer (SSL) protocol.

For more information, see *Transport Layer Security* in the *SAP NetWeaver* Security Guide.

Network Security

Use

Since *SAP Dispute Management* is based on the technology of *SAP NetWeaver*, for information about network security, see the following sections of the *SAP NetWeaver Security Guide*:

- **Network Services**

  This section contains information about services and ports that *SAP NetWeaver* uses.

- **Using Firewall Systems for Access Control**

  This section contains information about firewall settings.

- **Using Multiple Network Zones**

  This section contains information about which parts of your application should be set up in which network segments.

Communication Destinations

Use

The following table shows an overview of the communication destinations used by *SAP Dispute Management*.

Destination	Delivered	Type	User, Authorizations	Description
Example: DM2FIN_DIAG	No	RFC	Under Authorizations [Seite 11], you can see the roles for dialog users that you need for dialog calls that take place from the Dispute Case Processing system to the Accounts Receivable system.	This destination is used for dialog calls that take place from the Dispute Case Processing system to the Accounts Receivable system by means of RFC.
Example: DM2FIN_COMM	No	RFC	Under Authorizations [Seite 11], you can see the roles for communication users that you need for synchronous and asynchronous BAPI calls that take place from the Dispute Case Processing system to the Accounts Receivable system.	This destination is used for synchronous and asynchronous (IDocs) BAPI calls that take place from the Dispute Case Processing system to the Accounts Receivable system.

Example: FIN2DM_DIAG	No	RFC	Under Authorizations [Seite 11], you can see the roles for dialog users that you need for dialog calls that take place from the Accounts Receivable system to the Dispute Case Processing system.	This destination is used for dialog calls that take place from the Accounts Receivable system to the Dispute Case Processing system by means of RFC.
Example: FIN2COL_COMM	No	RFC	Under Authorizations [Seite 11], you can see the roles for communication users that you need for synchronous and asynchronous BAPI calls that take place from the Accounts Receivable system to the Dispute Case Processing system.	This destination is used for synchronous and asynchronous (IDocs) BAPI calls that take place from the Accounts Receivable system to the Dispute Case Processing system.

You can assign names for your RFC destinations as required. The names of the RFC destinations used above are merely examples.

When you set up the RFC destinations for the ALE scenario, check whether the option of trusted/trusting system relationship is relevant for you. Using an RFC trusted/trusting system relationship between two SAP systems means that in the case of an RFC (Remote Function Call) from the trusted to the trusting system, **no** password is sent for the logon to the trusting system. You can configure the RFC destinations in such a way that the call in the target system occurs with the current user from the calling system without a password being specified or entered on the logon screen. This has the following advantages, for example:

- When changes to objects or data are logged in the called system, this logging takes place with the current user from the calling system. This makes it easier to track changes that occurred through RFC.
- You can assign individual authorizations to the users in the called system. As such you can differentiate which actions or functions are accessible to the user in the called system irrespective of the user.

With this procedure, you must create the users that are to be allowed to execute using RFC functions in the called system as well. Note that in the ALE scenario of *SAP Dispute Management,* RFC calls take place from the Accounts Receivable system to the Dispute Case Processing system and vice versa. A trust relationship between SAP systems is **not** mutual. This means that you can choose whether one system is to be designated as trusted for the other system and vice versa, or whether you want to define the trust relationship only in one direction.

In the Customizing of ALE (Application Link Enabling), you can also define different RFC destinations for dialog calls, for BAPI calls, and for sending IDocs. As such you can also define an RFC destination for the dialog calls that use the trusted/trusting system relationship and use the current user from the calling system for the RFC calls in the target system, whilst you define an RFC destination for BAPI calls and for the sending of IDocs that does not use the trusted/trusting system relationship and in which you enter a communication user.

Note the following if your Accounts Receivable system is known as a trusted system by the Dispute Case Processing system and you want to configure the RFC destination used for sending IDocs so that it uses the trusted/trusting system relationship and the RFC calls in the target system with the current user from the calling system:

IDocs are sent to the Dispute Case Processing system from the Accounts Receivable system when items are cleared in the Accounts Receivable system, the clearing of items is reset, or partial payments are executed on items for which a promise to pay exists for the corresponding invoice. If the corresponding RFC destination uses the trusted/trusting system relationship, and carries out the call in the target system with the current user from the calling system, this means that the user triggering the clearing, reset of clearing, or partial payment must also be defined in the Dispute Case Processing system. You must therefore create **all** users who carry out clearings, reversals of clearings, or partial payments in the Accounts Receivable system, and therefore affect dispute cases, in the Dispute Case Processing system.

Data Storage Security

Use

Master data, transaction data, and Customizing data of *SAP Dispute Management* is stored in the database of the SAP system.

Access to the database is restricted by the authorization objects of *SAP Dispute Management*. To see the authorization objects relevant in *SAP Dispute Management*, see the roles listed under Authorizations [Seite 11].